RSAC 2025 Conference

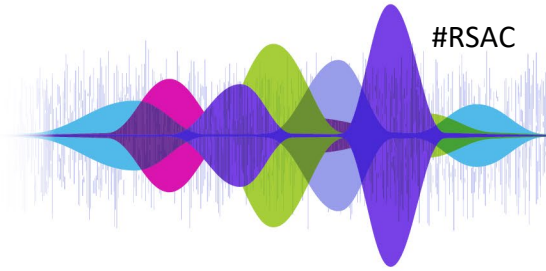
Many Voices.
One Community.

SESSION ID: FND-M03

Identity: The Last Bastion Security Control in a SaaS World

Aaron Turner

Faculty
IANS Research
https://www.linkedin.com/in/aaronrturner/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- Insights from the History of Identity Technologies
- Current State of the Identity Ecosystem
- Preparing for the Worst: 2025 Attack Paths
- Prioritizing Identity in the Age of AI
- Building Your Own Identity Roadmap

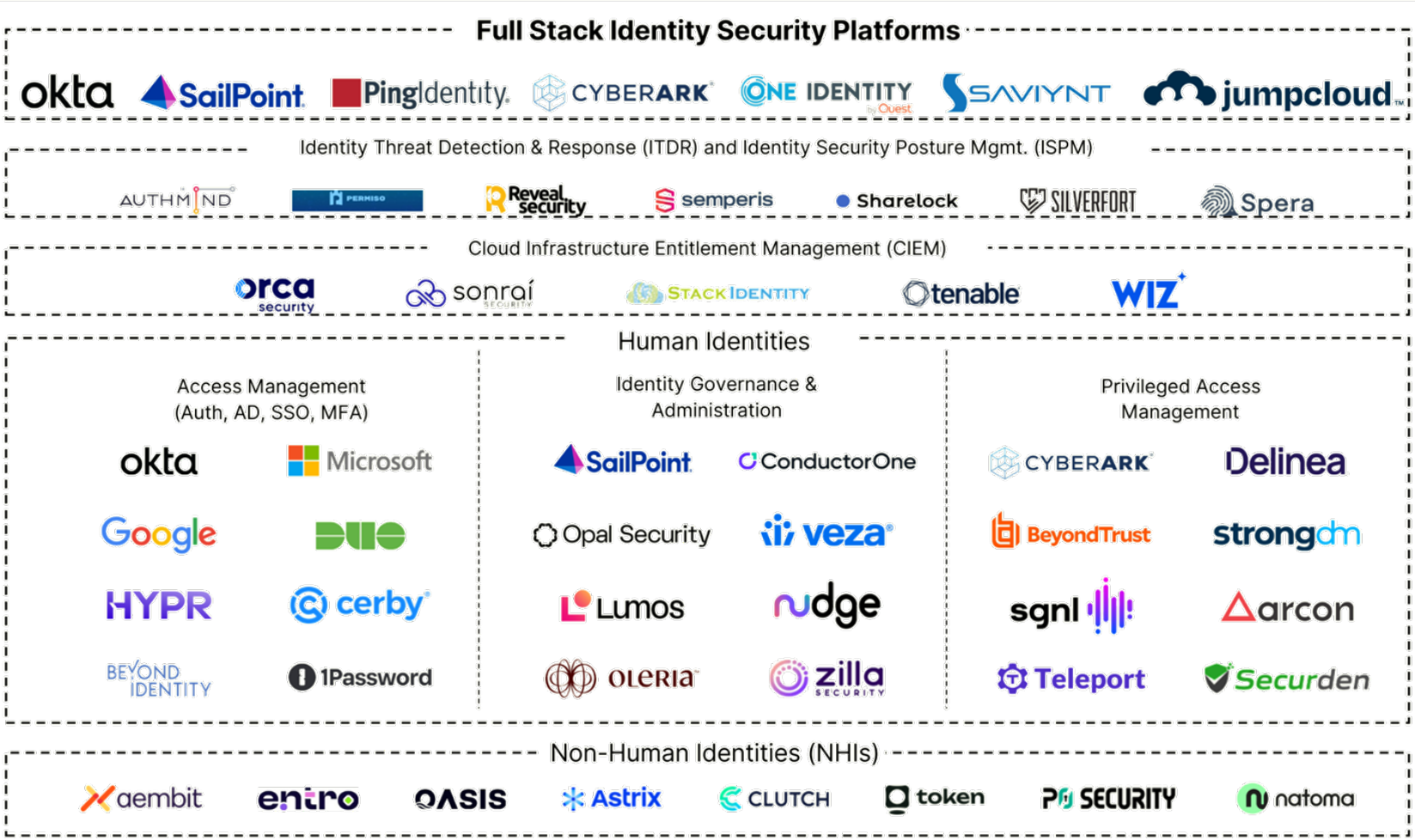
4 Decades of Identity Adoption Trends

1960s	**Passwords**	1990s	**Strong MFA**	Mid-2000s	**Privileged User Mgmt**	Mid-2010s
Usernames	1980s	**UNIQUE Usernames**	2000s	**Identity Governance**	2010s	**Single Sign On (IdPs)**

- 2000:
  - Firewall budgets were 1000X Identity budgets
- Active Directory warped the Identity market
  - “AD is my identity solution!”
- SaaS and AI have exposed 3 decades of atrocious under-investment
- Under-investment has created a gap in skills and availability of architects
- As IANS Faculty: 3000+ Identity and Access Management Consulting Calls since 2006

2025: State of the Identity Ecosystem

- Fragmented
- Lacking Economies of Scale
- Continued market warping due to Microsoft



https://www.madrona.com/workforce-identity-security/

Nation/State Identity Attacks: Diverse IdPs = Bad

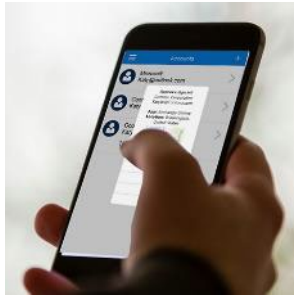
- The more identity platforms you have, the larger your identity attack surface
- REDUCE the number of IdPs ASAP
- For M365 organizations: Entra ID (especially eliminating on-prem AD)
- For non-M365 organizations: JumpCloud

https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF

2025 Identity Attack Path

Nation/State cyber team contracted with off-shore attacker groups with combination of **social media and infrastructure** skills targeting infrastructure operator

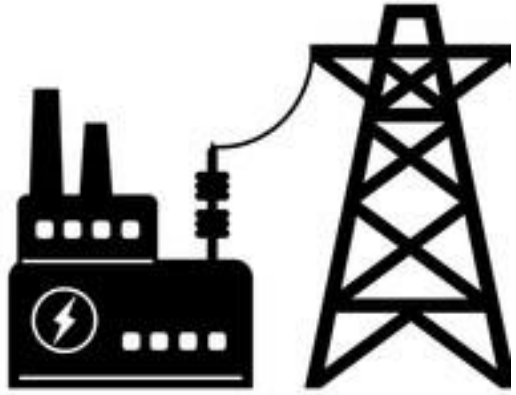
Purchased LinkedIn search results targeting **personal information** of operating engineers



Mobile phone numbers used to profile any personal mobile devices used for authentication for **mobile OS vulnerabilities and MFA auth cloning**

Personal email addresses used to send emails to obtain **IP addresses of home network**, profiling of home network equipment for **firmware vulnerabilities**

Attackers waited until **OT-destined VPN session** initiated and followed along, using home router as command-and-control connection

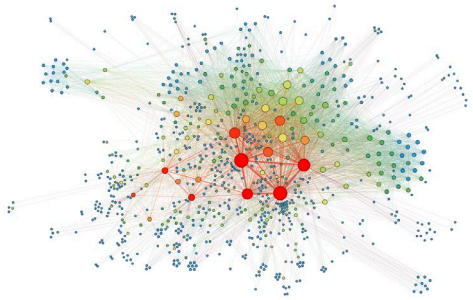


Compromised home router and personal device to target corporate-managed laptop

Prioritizing Identity in the Age of AI

- Eliminate legacy identities ASAP
  - Per-database, NTLM and Kerberos identities should be terminated ASAP
- OAuth is the future
  - Focus on end-to-end identities from data sources to analytics platforms to user interfaces
- Segment Knowledge Worker and Privileged User Identities
  - Most organization IT workers should have 3 identities
    - Daily driver (email, collaboration, etc.)
    - Legacy privileged account (preferably with a vaulting solution)
    - Cloud privileged account (preferably with a Yubikey and JIT privileges)

Building Your Own Identity Roadmap



- Assess ACTUAL identity protocol use across the organization
  - Network traces/PCAPs DO NOT LIE
  - https://gravwell.io
- Enumerate all identities used by knowledge workers as well as developers and administrators
  - PowerShell/Bash scripts are your friend
  - Goal is to achieve 1:1 mapping between every process in memory and a digital identity across the environment
- Cloud user accountability
  - Move to SSO ASAP, but in the interim use CSPM or other cloud visibility tools to understand the scale of the privileged user problem
- Developers Developers Developers
- Moving to modern Identity Providers is possible!

```
#!/bin/bash

# List all user accounts from /etc/passwd
echo "User accounts on this server:"
awk -F: '{ print $1 }' /etc/passwd

echo ""
echo "Last login times for each user:"
echo "--------------------------------"

# Check last login time for each user
awk -F: '{ print $1 }' /etc/passwd | while read user; do
    lastlog -u "$user"
done
```

Create Measurable Plans for Strategic Improvements

- Identity Governance:
  - Clean HR data goes a long ways to automating on/off-boarding
- Privileged User Management:
  - Driving discipline across admins and devs to require vaulted credentials pays huge dividends
- Federated Identities
  - Single Sign On and Passwordless reduce the risk of phishing and other credential theft

Go Make Identity Better In Your Organization!

- Can you partner with your network operations team to look at the use of identity authentication protocols?
- Can you work with your HR team to make sure that you have really solid ‘sources of truth’ for role based access control?
- Are there DevOps teams/processes that you can monitor for how privileges are used today for Dev/Test/Prod situations?
- What is the intersection of non-human identities and secrets and your current program capabilities? SSL Certs? SSH Keys?

Whichever Direction You Go…

- User identity information quality matters – clean it up whenever you can
- Non-human identities are generally the easiest to abuse – inventory them as soon as possible
- MFA exemptions are material regardless of what type of account – reduce those exemptions
- Reduce your identity attack surface whenever possible

Identity Roadmap Resources

- 4 Free IANS Research Whitepapers to help you navigate the identity landscape:
- Privileged Access Management
- Non-Human Identity Management
- Entra ID SSO Tips
- IAM Program Best Practices

https://iansresearch.com/resources/infosec-content-downloads

OR

https://iansresearch.com/RSAC2025

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You!